Preprint
UCRL-JC-143539-REV-1

Designing Remote Monitoring Systems for Long Term Maintenance and Reliability

G.E. Davis, G.L. Johnson, F.D. Schrader, M.A. Stone, E.F. Wilson

This article was submitted to
Symposium on International Safeguards: Verification & Nuclear Material Security, Vienna, Austria, October 29 – November 2, 2001

U.S. Department of Energy

Lawrence
Livermore
National
Laboratory

October 12, 2001

DESIGNING REMOTE MONITORING SYSTEMS FOR LONG TERM MAINTENANCE AND RELIABILITY *

G. E. Davis, G.L. Johnson, F. D. Schrader, M. A. Stone, E. F. Wilson
Lawrence Livermore National Laboratory
Livermore, California, United States of America

Abstract

As part of the effort to modernize safeguards equipment, the IAEA is continuing to acquire and install equipment for upgrading obsolete surveillance systems with digital technology; and providing remote-monitoring capabilities where and when economically justified. Remote monitoring is expected to reduce inspection effort, particularly at storage facilities and reactor sites. Remote monitoring technology will not only involve surveillance, but will also include seals, sensors, and other unattended measurement equipment.

The experience of Lawrence Livermore National Laboratory (LLNL) with the Argus Security System offers lessons for the design, deployment, and maintenance of remote monitoring systems. Argus is an integrated security system for protection of high-consequence U.S. Government assets, including nuclear materials. Argus provides secure transmission of sensor data, administrative data, and video information to support intrusion detection and access control functions. LLNL developed and deployed the Argus system on its own site in 1988. Since that time LLNL has installed, maintained, and upgraded Argus systems at several Department of Energy and Department of Defense sites in the U.S. and at the original LLNL site. Argus has provided high levels of reliability and integrity, and reduced overall lifecycle cost through incremental improvements to hardware and software. This philosophy permits expansion of functional capability, hardware upgrade and software upgrade without system outages and with minimum outage of local functions.

This presentation will describe Argus design strategies and lessons learned from the Argus program as they apply to the design, development, and maintenance of a remote monitoring network.

Hardware failures, software failures, and communication outages are expected and must be addressed by astute selection of system architecture. A combination of redundancy, diversity, and effective functional allocation between field and system level components should allow the system to tolerate component failures and communication interruptions. To the extent practical, field functions should continue to operate given communications interruptions or failure of central computers. Complete system functionality and history must be restored quickly after communications or central computer functions are restored. The needs for redundant functions to tolerate hardware failure and diverse functions to tolerate common cause (e.g., software errors) failures should be carefully evaluated and addressed in the system design.

Fundamental changes to communications backbone are expensive. Careful initial design of this feature is important to minimize the cost and system upset of future upgrades. The design

* This work was performed under the auspices of the U.S. Department of Energy by the University of California, Lawrence Livermore National Laboratory under contract No. W-7405-Eng-48.

should incorporate performance margin to support future functional enhancements and support open communications protocols that allow new types of equipment to be added to the system without significant changes. Any long-lived system will continually evolve. Therefore, hardware and software design must provide enhancement of capabilities and backward compatibility. Consideration of future system directions in design allows the system to evolve gracefully over time. This consideration requires a good understanding of customer needs and wishes and a strategic plan for system evolution. With this approach, significant enhancements in functionality and migration away from obsolete equipment can happen without the need for major system outages.

Upgrade of field units must be fast, simple, and secure. Storage of field software as firmware provides a high level of software security and allows "drop-in" software upgrade.

Argus software was designed with ease of modification and upgrade in mind. The product uses Ada for most of the software, taking advantage of its packaging and exception handling capability for effective organization of the software. Recent software has been developed using C++ and object-oriented design techniques to improve maintainability.

Secure communications does not necessarily require secure communications systems. Encryption and tamper detection features can assure a high level of data integrity over non-secure communications system. Security features must be readily upgradeable to allow improvement as the threats and the defenses become more sophisticated. A combination of hardware and software features can assure a high level of data integrity while supporting frequent enhancement.

The overall Argus system continues to support the capability for incremental modernization without complete system replacement since its initial installation in 1988. Several sites have upgraded host computers, field processors, console computers, and other significant system components. The system software is now in its 22nd major release with new functionality included with each release. Argus continues to be a robust security system, and the development team continues work on further modernization of software and system components.

1. Introduction

As part of the effort to modernize safeguards equipment, the IAEA is continuing to acquire and install equipment for upgrading obsolete surveillance systems with digital technology and providing remote-monitoring capabilities where and when economically justified. Remote monitoring is expected to reduce inspection effort, particularly at storage facilities and reactor sites. Remote monitoring technology will not only involve surveillance, but will also include seals, sensors, and other unattended measurement equipment.

1.1 Argus Success With Remote Monitoring

LLNL's experience with the Argus Security System offers lessons for the design, deployment, and maintenance of remote monitoring systems. Argus is an integrated security system for protection of high-consequence U.S. Government assets, including nuclear materials. Argus provides secure transmission of sensor data, administrative data, and video information to support intrusion detection and access control functions.

LLNL developed and deployed the Argus system on its own site in 1988. Since that time, LLNL has installed, maintained, and upgraded Argus systems at several Department of Energy and Department of Defense sites in the U.S. and at the original LLNL site. Argus has provided high levels of reliability and integrity, and reduced overall lifecycle cost through incremental improvements to hardware and software. Key upgrades to the Argus system include the system operator Consoles (1993), host computer systems (1993 and 2000), communications/network (1995), field processor (1995), and key system configuration tools (2001). Upgrades are currently in progress for the system operator Consoles, database, field processor, video recorders, and additional configuration tools. This philosophy permits expansion of functional capability, hardware upgrade and software upgrade without system outages and with minimum outage of local functions.

1.2 Argus Application Similarities to Remote Monitoring Application

Automated security systems and remote monitoring systems share a fundamental function: to collect video and sensor data from a large number of points and send this information to centralized locations for interpretation and processing. Argus cameras and sensors are distributed on sites that cover many square miles. National level monitoring of multiple sites is known to be feasible. The sites covered by the Argus systems are similar to, but typically larger than, those of facilities in the nuclear fuel cycle. However, international-level monitoring of a large number of sites will be needed.

Both systems must be capable of time-correlating video and other sensor information. Information processing is necessary in both cases to detect and alert operators to unusual conditions present in a high volume of data. In addition to the common functional requirements, certain other design goals are common.

- **Tamper resistance:** It should be difficult to tamper with field devices. Deception of field devices and injection of false data at field devices or along communications networks should always be detectable.

- **Dependability:** Individual component or communications failures should be readily detectable and should not cause failure of critical functions. In the event of complete communications failure, local devices should continue to perform critical functions and update central locations when communications are restored.

- **Low cost:** Production, installation, and operational costs must be low enough that organizations can afford to deploy and maintain a large number of field units.

- **Maintainable:** Maintenance and upgrade of equipment and software must be possible without interrupting key functions.

1.3 Factors in Argus Remote Monitoring Success

The Argus security system has become a proven success because of a number of factors. These same factors can be applied to the remote monitoring problems of IAEA. First, Argus was designed as an integrated system with well-defined requirements. The initial requirements for the system evolved from U.S. Department of Energy Orders and Directives, input from experienced LLNL Security and Maintenance personnel, and Department of Energy and LLNL managers responsible for the project. Key factors such as reliability, maintainability, continuity of operation, and ongoing upgrade capability were clearly specified in the initial requirements. Second, Argus was designed as an open, evolutionary system, as opposed to a static system. This feature, along with an active R&D and software maintenance effort, permits the addition or replacement of components and functionality to add capability and prevent obsolescence. Third, Argus managers enforced quality standards, project management, implementation standards for the addition of new sites, and a focus on customer satisfaction for ongoing support.

The use of open standards and an evolutionary approach to system support has kept Argus aligned with current technology during its fourteen years of operation. New Argus sites installed in 2001 take advantage of current changes to the system design and receive the current Argus software releases. Minor software updates are released every three to six months. A minor software release involves one or more Argus software products and usually involves a combination of bug fixes and new software features. Major software updates are released every one to two years. A major software release incorporates previous minor releases to Argus software products and usually involves one or more major additions to Argus software functionality.

Hardware changes to the Argus system are infrequent compared with software changes. Typical replacement cycles are five years for host computers, ten years for operator display consoles, field processors, video equipment, and network/communications equipment. Commercial equipment is typically used except for field processors, which are designed to meet demanding environmental requirements. All upgrades and enhancements must offer enhanced or modernized capability, as well as being backward compatible with the existing system. Existing equipment is supported until all Argus customers complete equipment replacement at their site. A significant point about system upgrades is that they do not require replacement of the entire system and supporting infrastructure at the same time. Argus systems were typically installed in facilities with modest expansion capacity and are interconnected using quality cable and fiber optic plant. System design engineers do not expect to replace these parts of the system in the foreseeable future.

2. Overall Security Strategy

Argus was designed with an overall security strategy in mind. It was designed from inception as a security system for high-consequence applications. System engineers not only focus on current U.S. Department of Energy and Department of Defense orders and directives, but also begin implementation of pending orders and directives as they are announced.

The Argus system contains numerous features for enhanced security applications. Many of these features are applicable to IAEA remote monitoring applications. Argus' hierarchical structure of host and sub-host computers, communication concentrators, and field processors permits a geographically distributed system of almost unlimited size. It permits central or distributed monitoring of system alarms and video display. The Argus system features integration of sophisticated personnel access control and intrusion detection capability. The access control capability improves the accuracy of personnel recognition at a facility entry point while reducing the cost of security force labor. Other key system features include central or distributed alarm station control and access privilege control by security administrators and designees, tamper and environmental monitoring of system components, and encrypted communications to prevent insertion of surrogate equipment at a remote site.

2.1 System Design Approach

A system design approach, addressing physical conditions as well as human factors, allows new or changed functionality to be accommodated at multiple layers of a system. Argus has been successful at adapting to changes of hardware and functional requirements because of its ability to migrate functionality between levels of the hardware architecture. When components with fixed functionality are simply integrated, the system built is the lowest common denominator of all pieces assembled. The general design requires remote processing capable of autonomously handling all uncoordinated events. A minimal number of events may require coordination between either multiple remote processors or between one remote and a host computer or dispatcher. This minimizes the impact on communications.

As a general guide, the N+1 rule for redundancy applies: one more of any component at any point in the system is needed (for redundancy) than is required to fully operate the system. For example, if the command center requires a single uninterruptible power supply and backup generator to operate at capacity, then two of each must be provided. Host computers, networks, secure communications paths, data storage, dispatcher consoles, etc., should all be designed with N+1 or greater redundancy. Dynamic fault detection can further improve reliability.

Environmental constraints including operating temperature range, rate of temperature change, lightning, humidity, altitude, sunlight, electro-magnetic fields, penetrating radiation, and availability of clean electric power all impact performance, reliability, and component lifetime. Careful design, prototyping, and testing can produce more robust components with higher initial cost but lower total cost of ownership.

Designing maintenance friendly features into hardware and software can also work toward decreasing total cost of ownership of a system. Hardware designs should allow rapid replacement and startup of Field Replaceable Units (FRUs). Visual indicators with good diagnostic manuals can greatly reduce Mean-Tine To Repair (MTTR) numbers for a system and the level of training and expertise required by field technicians.

A design that utilizes a single basic set of hardware and software, configurable to meet multiple requirements, can further reduce overall costs. If a feature is supported but not currently used at one site becomes necessary there, it can simply be enabled without the need to add other unique components. Designs that utilize many diverse components require all of those unique pieces to be designed, tested and maintained, usually at much greater total cost of ownership.

2.2 Ongoing Support of Remote Monitoring Systems

To ensure a long life, technical security systems require a strategic planning process, technical resources, and funding to support system upgrades. Since upgrade possibilities are endless and financial resources are limited, the selection, implementation, and staging of upgrades are critical to the system's long-term success. The Argus team breaks upgrades down into three categories:

- Viability
- R&D
- Site-specific

Viability upgrades are identified by the technical staff and are modifications required to keep the system technologically current so that systems can continue to be operated, produced and installed. Viability upgrades are not intended to add new features or capabilities to the system. An example of a viability upgrade would be modifications required to replace an obsolete computer with a commercially available replacement. Another example would be the modifications required to support a new version of an operating system.

The DOE Headquarters technology development program staff identifies R&D upgrades after reviewing proposals from the National Laboratories in response to general user needs and threat assessments. These two to four year projects are aimed at increasing the overall capability through changes or additions to the system. An example of an R&D upgrade would be the development of an intelligent sensor system or the incorporation of digital video into the system. Site-specific upgrades are identified by the user community and are highly targeted requests for specific system changes or enhancements to address conditions at their sites. Site-specific modifications must be carefully handled to prevent unintended impacts to system operation at other sites. An example would be the integration of a site-required subsystem into the Argus system such as a site's badging or employee information management system.

The viability and R&D upgrades are focused on improving the entire Argus system while the site-specific upgrades create features that are typically used by one or two sites. It is important to get feedback from upgrade sponsors to ensure that the development team is producing the right product. Formal Technical Interchange Meetings, Quality Panels, Program and Project Reviews are held throughout the year. In addition, a single point contact or "site liaison" is responsible for communicating with each site and a System Performance Report database is maintained to capture customer concerns and to allow the Argus staff to track the resolution of problems and implementation of enhancements.

It is also important to support R&D and viability projects from a team management perspective. Developing new security technologies on current systems is a powerful attractor of high caliber technical talent. This is particularly important for an organization that lives on the border of Silicon Valley.

2.3 Software Design for Maintainability

Argus software is designed for maintainability. Host and embedded software is predominantly written in Ada, and PC user interface software is written using Rapid Application Development (RAD) C++ tools. It is our general view that the Ada software environment is better suited for long-term maintenance and stability, whereas the RAD tools better support the frequent upgrades in the PC user interface environment.

The Ada software is developed using object-oriented techniques, and reusability is a major driver. Whenever a new software module is added, an evaluation is made as to how the module can be written for future reuse. This adds a small cost for a given module, but the technique generates a large library of reusable, domain-applicable modules, which reduce overall cost and schedule of software enhancements. Each Ada module has a standalone test application, which developers use to debug the module before integration with the rest of the application. When enhancements are made to a module, the test application is updated accordingly, and is used for both new feature and regression testing.

The object-oriented approach lends itself to a long-lived evolving system. For example, the host communications was originally implemented using DECnet, a proprietary network package for VMS. Two Ada modules were written to support the use of DECnet – a server module and a client module – and the interfaces were independent of the specifics of DECnet. With the introduction of PCs as user interface machines, much of the network has migrated to TCP/IP. We were able to change the implementation of the two Ada modules to support both DECnet and TCP/IP, and none of the dozens of applications using these modules needed any change at all to take advantage of the new TCP/IP functionality.

Argus features are also designed for maintainability. When a user requests a new feature, the feature is often generalized into a feature class. This feature class is implemented, usually in association with the Argus configuration database, which directs the software how to operate at a given site. An example of this is the requirement for multi-person rule for maintenance operations at field panels. One site wanted the system to enforce the presence of two maintenance users to enter "maintenance mode". The implementation of this feature extended the requirement to "n-person" rule and allowed other roles than maintenance to be required. The sites use the database to define these rules on an area-by-area basis. This capability has been used extensively at each Argus site to tune the operation of their system to their specific security needs.

2.4 System Testing and Quality Approach

The Argus team takes a high quality approach to the release of software and hardware before site use. All software releases are tested at LLNL on an isolated test system by a dedicated test team. The test system is designed to simulate all major field configurations. It also includes supported legacy equipment for backward compatibility testing. System tests are primarily performed manually at this time. Automated testing of software is expected to reduce release time and improve software quality in the next two to three years. All software released after completion of testing is under configuration control at LLNL.

Argus engineers require significant testing of hardware and systems before site use. All new field hardware is subjected to environmental qualification. This testing includes lightning immunity tests, low and high temperature tests, and tests at altitudes of up to 10,000 feet. Special versions of equipment can be built with radiation-hardened components and qualified for use in radiation environments, using LLNL expertise developed through spacecraft electronics programs.

All equipment manufactured by LLNL for customer sites is subjected to incoming inspection, manufacturing tests, and burn-in of completed units to avoid infant mortality failures. New Argus systems are integrated at LLNL and loaded with current software. Following this integration effort, the customer site is invited to come to LLNL to witness the pre-installation acceptance tests.

The successful deployment of Argus to customer sites is handled by project teams based at LLNL. The effort begins with a conceptual design effort, usually required for project funding proposals. When the project is funded, Argus management assigns a dedicated project manager and project engineer to design, procure, and install the system at the customer site. The project operates in a formal fashion, similar to U.S. commercial contracts. The project team members exchange information with their counterparts via weekly teleconferences, electronic mail, and formal requests for information and responses. Face-to-face meetings occur monthly and usually coincide with design reviews or lengthy technical discussions. The project schedule and financial controls are managed using Primavera Enterprise software. This software provides monthly earned- value reporting of cost and schedule variances.

In addition to the assembly and installation of the system, the project typically includes onsite training of users. Training includes classroom training, on-the-job training, and computer-based training. Once the site users are trained, they are qualified to witness the formal acceptance test of the system at LLNL. They perform the final acceptance test of the system following installation at the site. Formal closeout of the project includes a project closeout document, final project cost report, closeout of all cost accounts at LLNL, and return of any remaining funds to the customer site.

3.0 Summary

The Argus system and its design experiences provide an excellent approach for IAEA in planning and implementing remote monitoring systems. Some of the factors in Argus remote monitoring success include its design as an integrated system, its design as an open, evolutionary system, and management focus on quality, project management and customer satisfaction. As a measure of Argus' successful approach, several customer sites have upgraded host computers, field processors, console computers, and other significant system components since initial installation. The system software is now in its 22nd major release, with new functionality included with each release. Argus continues to be a robust security system, and the development team continues work on further modernization of software and system components.